PUBLIC KEY INFRASTRUCTURE MASTER KEY

Philip J. Mire

ABSTRACT OF THE DISCLOSURE

The invention encrypts and decrypts data using public key infrastructure with and allows an authorized third party to access and decrypt the encrypted data as required without requiring private key escrow. The invention utilizes a user private key, a user public key, a master private key, a master public key, and a session key generated by the system. The data is encrypted utilizing the session key. The session key is encrypted once utilizing the user public key and again utilizing the master public key. The encrypted data and the encrypted session keys are included in a data packet that is transmitted from one data processing system to another. The session key is decrypted utilizing the user private key. The data is decrypted utilizing the session key. When the authorized third party requires access to the data on the destination processing system, the session key is decrypted with the master private key and the data is decrypted with the session key.